UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,979	04/19/2001	Peter V. Radatti	16-00	1266

7590 02/09/2006

CyberSoft, Inc.
1508 Butler Pike
Conshohocken, PA 19428

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 02/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/838,979	RADATTI, PETER V.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/07/05 has been entered.

Response to Arguments

Applicant's arguments filed 03/23/05 have been fully considered but they are not persuasive because of following reasons.

The affidavit filed on 03/23/2005 under 37 CFR 1.131 has been considered but is ineffective to overcome the Jordan (20020073323) reference.

The evidence submitted is insufficient to establish a conception of the invention prior to the effective date of the July 14, 2000 reference. While conception is the mental part of the inventive act, it must be capable of proof, such as by demonstrative evidence or by a complete disclosure to another. Conception is more than a vague idea of how to solve a problem. The requisite means themselves and their interaction must also be comprehended. See *Mergenthaler v. Scudder*, 1897 C.D. 724, 81 O.G. 1417 (D.C. Cir. 1897).

The applicant argues that "...writing the results of the interpretation..." is at least inherent in the build up. However, the definition of build up is to develop gradually by

increments. There is no writing process involved in building up. Therefore, the evidence provided does not disclose step of "writing the results of said interpretation," as claimed in claim 1. The reference to build up suggests the development of the translation of the set of steps of the Macro Interpreter.

The applicant argues further, "... the interpreter is what interprets - and macros are code. Thus, the presence of a macro interpreter provides the disclosure showing that code is interpreted..." However, the definition of Macro is a set of keystrokes and instructions recorded and saved under a short key code or macro name. When the key code is typed or the macro name is used, the program carries out the instructions of the macro. Therefore interpreting a set of keystrokes does not equate to interpreting code.

The applicant argues further that the reference to macro interpreter should be taken as a showing of computer readable media because Macros are generally contained upon computer readable medium and are interpreted during a read from that media. However, the applicant earlier disclosed Macro interpreter as a code interpreter, this does not indicate an interactions with computer readable media.

In reference to the applicants arguments that the manager is asked to make a decision after the virus scan reports and further the good/no good designation provides a result evaluator as well as a reporter. A manager by definition is a person whose work or profession is management. The claim preamble discloses a software virus detection apparatus that comprises, among other things, an evaluator. The applicant discloses that the manager is the evaluator. The applicant does not disclose how the apparatus will comprise a person whose work or profession is management. Furthermore, the good/ no good designation is supposed corresponds to the

reporter as disclosed by the applicant. The definition of reporter is a report generator which is an application commonly part of a database management program that uses a report form created by the user to lay out and print the contents. The designation good/ no good does not suggest creating a report form and printing the contents.

With the above discussion in mind, the applicant has not provided proof of conception such as a complete disclosure (emphasis added). Instead, the applicant has provided a vague idea of how to solve a problem.

In reference to the applicant's affidavit properly and clearly reciting that due diligence was exercised, this is a conclusive statement that does not provide factual support.

The evidence submitted is insufficient to establish diligence from a date prior to the date of reduction to practice of the Jordan reference to either a constructive reduction to practice or an actual reduction to practice.

What is meant by diligence is brought out in Christie v. Seybold, 1893 C.D. 515, 64 O.G. 1650 (6th Cir. 1893). In patent law, an inventor is either diligent at a given time or he is not diligent; there are no degrees of diligence. An applicant may be diligent within the meaning of the patent law when he or she is doing nothing, if his or her lack of activity is excused. Note, however, that the record must set forth an explanation or excuse for the inactivity; the USPTO or courts will not speculate on possible explanations for delay or inactivity. See In re Nelson, 420 F.2d 1079, 164 USPQ 458 (CCPA 1970). Diligence must be judged on the basis of the particular facts in each case. See MPEP § 2138.06 for a detailed discussion of the diligence requirement for proving prior invention. Under 37 CFR 1.131, the critical period in which diligence must be shown begins just

prior to the effective date of the reference or activity and ends with the date of a reduction to practice, either actual or constructive (i.e., filing a United States patent application). Note, therefore, that only diligence before reduction to practice is a material consideration. The "lapse of time between the completion or reduction to practice of an invention and the filing of an application thereon" is not relevant to an affidavit or declaration under 37 CFR 1.131. See Ex parte Merz, 75 USPQ 296 (Bd. App. 1947).

Applicant should provide, in an Affidavit, a detailed description from conception date (December 15, 1999) to the filing date. Applicant should also see MPEP 2138.06 and 2138.06.

Therefore Jordan will not be withdrawn as a reference.

The applicant argued that applicant is unable to fine anywhere in Jordan any mention of scanning any results of any interpretation. This is not found persuasive. In Fig. 3 discloses a detector component that would receive data from the emulator and the monitor. The detector by definition discovers the true character of the code. The discovery of the true character of the code requires examination of the code and therefore scanning.

The applicant argued further that the applicant finds no reference to an interpreted table in Jordan. This is not found persuasive. The applicant's claim 6 does not disclose an interpreted table, instead the claim recites a table of interpreted results. The element, in the reference of Jordan, that corresponds to the table of interpreted results is the information regarding the emulated code sent from the monitor to the detector corresponds to the table of interpreted result. The result may be presented in the form of a table for convenience.

The applicant argues that one cannot see the equivalent to claim 7's reporter and evaluator. The detector of Fig. 3 determines the true nature of the code as discussed above and is therefore the evaluator and then it reports the results as suggested in Fig. 1.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5

USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, patterns are a simple way of defining deviation from the normal operation of the system the system of Jordan is used to detect viruses which are a deviation from the normal operation of computer code as a result the method of Shieh is a simple method of defining the deviations.

Claim Rejections - 35 USC § 103

Claims 1-4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan (2002/0073323 A1).

In reference to claim 1 and 6, Jordan discloses a system and method for detecting computer viruses that attempt to gain access to restricted computer (abstract). The method includes writing the results and scanning the results for the presence of proscribed code (page 3 paragraph 0028).

Although Jordan does not expressly disclose interpreting code, Jordan discloses an emulator that emulates the executable code (page 3 paragraph 0028).

Afzal discloses an emulator that is an instruction-by-instruction interpreter (page 145 Introduction paragraph 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the emulator to perform the function of the interpreter. One of ordinary skill in the art would have been motivated to do this because it is desirable that the malicious code is not executed and the interpreter and the emulator do not execute the code, instead they simulate the execution of the code.

In reference to claim 2, wherein scanning the results of said interpretation for the presence of proscribed code further comprises scanning for the presence of code of interest. Jordan discloses detecting modification of memory (page 3 paragraph 0027) and therefore code of interest.

In reference to claim 3, wherein the first scanning step for the presence of code of interest further comprises scanning for a file open command or a file modify command. Jordan discloses detecting modification of memory (page 3 paragraph 0027). Modifying a file will modify memory.

In reference to claim 4, wherein the step of scanning further comprising a second scanning step for the presence of proscribed code of interest. Jordan discloses detecting modification of memory (page 3 paragraph 0027), the access of memory includes accessing restricted computer system resources; this is the presence of proscribed code.

Claims 5, 7-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jordan as applied to claim 1, and 4 respectfully above, and further in view of Shieh et al (5,278,901).

In reference to claim 7, is rejected as in claim 1 a system and method for detecting computer viruses that attempt to gain access to restricted computer (abstract). The method includes interpreting code (emulator) that emulates the executable code (page 3 paragraph 0028), a reporter and a results evaluator (page 3 paragraph 0028), whereby the file is interpreted by the emulator and results generated those results sent to the evaluator (detector) that determines if malicious code is present and then the results are reported. However Jordan does not expressly disclose a pattern analyzer.

However Shieh discloses a pattern-oriented system and method of intrusion detection (column 4 lines 9-22). The pattern-oriented system is used to detect virus propagation (column 16 lines 31 to column 17 line 30); therefore the pattern analyzer reviews patterns for the presence of proscribed code.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a pattern analyzer for detection for intrusion detection as in the system by Shieh in the system of Jordan. One of ordinary skill in the art would have been motivated to do this because patterns are a simple way of defining deviation from the normal operation of the system.

Although Jordan does not expressly disclose interpreting code, Jordan discloses an emulator that emulates the executable code (page 3 paragraph 0028).

Afzal discloses an emulator that is an instruction-by-instruction interpreter (page 145 Introduction paragraph 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the emulator to perform the function of the interpreter. One of ordinary skill in the art would have been motivated to do this because it is desirable that the malicious code is not executed and the interpreter and the emulator do not execute the code, instead they simulate the execution of the code.

In reference to claim 5, Jordan does not expressly disclose a system wherein the second scanning step for the presence of proscribed code of interest further comprises scanning for viral code or viral patterns.

However Shieh discloses a pattern-oriented system and method of intrusion detection (column 4 lines 9-22).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use pattern detection for intrusion detection as in the system by Shieh in the system of Jordan. One of ordinary skill in the art would have been motivated to do this because patterns are a simple way of defining deviation from the normal operation of the system..

In reference to claim 8, wherein the step of scanning further comprising a first scanning step for the presence of code of interest. Jordan discloses detecting modification of memory (page 3 paragraph 0027) and therefore code of interest.

In reference to claim 9, wherein the first scanning step for the presence of code of interest further comprises scanning for a file open command or a file modify command. Jordan discloses detecting modification of memory (page 3 paragraph 0027). Modifying a file will modify memory.

In reference to claims 10-12, Jordan does not expressly disclose the pattern analyzer further reviews said code for the presence of code of interest.

Shieh discloses the pattern analyzer reviews code for the presence of problems, or code of interest (column 4 line 60 to column 5 line 11).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use pattern detection for code of interest as in the system by Shieh in the system of Jordan. One of ordinary skill in the art would have been motivated to do this because patterns are a simple way of defining deviation from the normal operation of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Sunday, February 05, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100